Bad Rabbit, la tercera oleada de ataques ransomware en 2017

Europa ha sido víctima de un nuevo ataque de ransomware. Tras Wannacry y ExPetr, que causaron pérdidas de cientos de millones de dólares, ahora hace su aparición en escena **Bad Rabbit.** La mayoría de las víctimas de este ataque se ubican en Rusia, aunque se han detectado casos "similares, pero en menor cantidad", en países como Turquía, Alemania o Ucrania. Como ha sucedido con otros ciberataques, el ransomware Bad Rabbit encripta determinados ficheros y exige el pago de una cantidad económica por su recuperación. En este caso, este gusano solicita el pago de 0,05 Bitcoins.

Bad Rabbit, datos más relevantes

- **Bad Rabbit tiene una clara conexión con el ataque de ExPetr** que tuvo lugar el pasado mes de junio de este año.
    - El mensaje pidiendo dinero está redactado de forma similar al que Expetr enviaba a sus víctimas
    - Ambos programas es que usan una versión personalizada de la herramienta para recuperar contraseñas Mimikatz y la red SMB para propagarse entre los equipos de una misma red.
    - El algoritmo hash utilizado en el ataque es similar al utilizado por ExPetr. Además, los expertos han detectado que ambos ataques utilizan los mismos dominios
    - En total, los programas **comparten un 67% del código**, aunque esto no es ninguna garantía de que el mismo grupo sea responsable de ambos ataques.
    - Al igual que exPetr, Bad Rabbit intenta hacerse con credenciales de la memoria del sistema y difundirse dentro de la red corporativa por WMIC. Sin embargo, los analistas no han encontrado los exploits EternalBlue o EternalRomance en el ataque del Bad Rabbit

- **Preparándose desde julio de 2017**. La investigación muestra que los ciberatacantes que están tras esta operación se han estado preparando al menos desde julio de 2017, creando su red de infección en sitios hackeados, principalmente medios de comunicación y recursos de información de noticias.

- Según la investigación de Kaspersky Lab, **Bad Rabbit ha afectado casi a 200 objetivos**, ubicados en Rusia, Ucrania, Turquía y Alemania. Todos los ataques tuvieron lugar el 24 de octubre, y no se han detectado nuevos ataques desde entonces. Los atacantes comprometieron varios sitios conocidos para difundir la amenaza. Los usuarios descargaban el programa malicioso creyendo que estaban instalando Flash Player; después se los dirigía

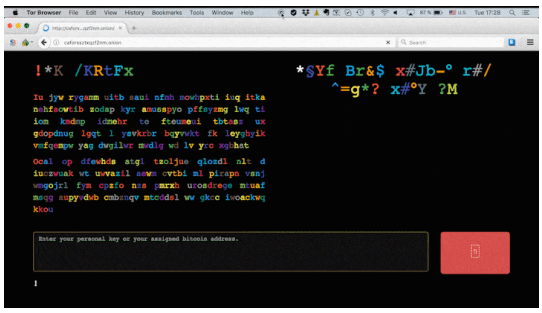
al sitio infectado con una descarga drive-by. Entre los sitios comprometidos se encontraban conocidos medios de comunicación de Rusia. Una vez que Bad Rabbit irrumpía en la red, se multiplicaba y expandía con funcionalidades de gusano.

- El ataque todavía no está muy expandido geográficamente: **se ha detectado un 65% de los ataques en Rusia y un 12,2% en Ucrania**. El resto de los ataques se encontró en otros países del este europeo, además de Turquía y Japón.

- Los servidores que los atacantes usaban para llevar a cabo el ataque se eliminaron de la red sólo seis horas después de que el programa comenzara a difundirse. De este modo se controló la amenaza incluso antes de que lograra cruzar al continente americano.

- **Los productos de Kaspersky Lab detectan el ataque desde el inicio y con éxito el ransomware**. Puede consultar el vídeo: https://www.youtube.com/watch?v=ZeZ9C8aPWtc&t=3s

Protégete



Para hacer frente a las ciberamenazas, hemos puesto a disposición de las empresas la **herramienta gratuita Kaspersky Anti-Ransomware Tool** para protegerse del ransomware y del cryptomalware. A través de esta solución de seguridad las compañías que no cuentan con soluciones de Kaspersky Lab puedan utilizar tecnologías avanzadas antiransomware. Esta herramienta incluye el componente SystemWatcher que detecta actividades sospechosas, crea una copia de respaldo temporal de archivos y revierte los cambios maliciosos, dejando el sistema intacto.xzz

Igualmente, y para proteger a usuarios y empresas, Kaspersky Lab, junto con Europol, la policía holandesa y otras empresas de ciberseguridad puso en marcha, hace un año, el proyecto **No More Ransom**. Esta iniciativa pretende luchar contra el auge de este tipo de ciberamenaza. Tras un año de actividad, ya cuenta con 109 partners y 54 herramientas de descifrado, abarcando 104 familias de ransomware. Gracias a estas herramientas se ha ayudado a descifrar más de 28.000 dispositivos. Durante su lanzamiento ha recibido más de 1,3 millones de visitantes únicos, recibiendo récord de visitas (150.000) en el mes de mayo, durante la crisis de WannaCry.

Algunos consejos

- Bloquear la ejecución de los archivos c:\windows\infpub.dat y c:\Windows\cscc.dat.
- Desactivar el servicio WMI (si es posible en tu entorno) para prevenir que el malware se extienda por tu red.
- Hacer copias de seguridad de los datos.
- Mantener actualizados los sistemas y programas
- No pagar el rescate
- Y, concretamente en el caso de usuarios de Kaspersky Lab, asegurarse de que tienen activados tanto System Watcher como Kaspersky Security Network.

Más información

https://securelist.com/bad-rabbit-ransomware/82851/

https://go.kaspersky.com/Ransomware.es.html

www.nomoreransom.org/es/index.html